Exhibit A

MICHAEL THOMSON 809 E. Broadway Bel Air, MD 21014, On behalf of himself and all others similarly situated, Plaintiff, v. MARRIOTT INTERNATIONAL, INC. 10400 Fernwood Road Bethesda, MD 20817, and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC, 10400 Fernwood Road Bethesda, MD 20817, Defendants.	IN THE CIRCUIT COURT FOR MONTGOMERY COUNTY, MD Case No ____________________ (JURY TRIAL DEMANDED)

CLASS ACTION COMPLAINT

Plaintiff Michael Thomson ("Plaintiff"), individually and on behalf of the Class and Subclasses of similarly situated persons defined below, alleges the following against Defendants Marriott International, Inc. ("Marriott International") and Starwood Hotels & Resorts Worldwide, LLC ("Starwood," and, together, "Marriott" or the "Company"), based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Marriott arising out of a massive data breach in which Marriott breached its duty to secure and safeguard its customers' sensitive personal, demographic, and financial data—including, but not limited to, names, addresses, phone numbers, email addresses, passport numbers, hotel reward account information, dates of birth, information regarding arrival and departure, reservation dates, communication preferences, and credit card numbers and expiration dates ("Personal Information")—and failed to provide clear, conspicuous, and timely notice to Plaintiff and the other members of the Class and Subclasses defined below that their information had been compromised.

2. On November 30, 2018, more than ten weeks after it had "received an alert from an internal security tool" regarding an unauthorized attempt to access the guest reservation database for certain Marriott-affiliated hotels in the United States, Marriott disclosed to the public that its systems were subject to one of the largest data breaches in our nation's history (the "Data Breach"). Shockingly, Marriott's investigation of the Data Breach revealed that the unauthorized access began occurring over **four years ago** in 2014 and had remained undetected and unaddressed until November 2018.

3. During the approximately four-year period between the initial breach and its discovery, a hacker or hackers took advantage of glaring weaknesses and vulnerabilities in Marriott's systems to steal the Personal Information of approximately **500 million individuals** who had stayed at certain Marriot-affiliated hotels during that period. For approximately four years, Marriott failed to detect the hackers' presence, notice the massive amounts of data that were being exfiltrated from its database, or take any steps to investigate the numerous red flags that should have warned the Company about what was happening.

4. Marriott has publicly acknowledged that the Data Breach resulted, at least in part, from faults in a database containing information of guests at its Starwood-branded hotels (the "Starwood Database"),[1] noting in an 8-K filed on November 30, 2018 that it was "devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to [its] network." The opportunities that any such faults created for hackers were greatly enhanced by Marriott's systemic incompetence and a longstanding, lackluster approach to data security that permeated the company's culture from the top down. Indeed, Marriott failed to employ sufficient security measures to avoid the Data Breach despite the fact that Starwood Hotels & Resorts Worldwide, Inc.—which Marriott International acquired in 2016 and whose database it admitted to have been compromised in the Data Breach—had reported a data breach relating to 54 of its hotels in November of 2015. Despite this data breach, as well as numerous other high-profile data breaches at other major American corporations (including Equifax and Target) during the four years between the initial breach and its discovery, Marriott took no steps to assure that its systems were secure.

5. Marriott had an independent duty to implement reasonable and adequate data security practices and affirmatively represents on its website that it subscribes to the EU-U.S. and Swiss-U.S. Privacy Shield programs and is committed to adhering to governing Privacy Shield Principles, which require "[o]rganizations creating, maintaining, using or disseminating personal information" to "take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destructions."

---

[1] Starwood brands include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels, as well as Starwood-branded timeshare properties.

6. However, Marriott's data security practices were neither reasonable nor appropriate, and were not in accord with industry standards. Marriott thus enabled hackers or other unscrupulous individuals or organizations to use information obtained as a result of Marriott's inadequate data security practices to exploit and injure Plaintiff and the members of the Class and Subclasses defined below. Exacerbating these injuries, Marriott failed to timely disclose the Data Breach or timely notify each affected customer. By failing to notify any customers until approximately four years after the initial breach (and more than ten weeks after Marriott claims to have first discovered a breach), Marriott prevented Plaintiff and other class members from adequately protecting themselves from its consequences.

7. Accordingly, Plaintiff, individually and on behalf of all other members of the proposed Nationwide Class (defined below), asserts claims against Marriott for negligence, breach of contract and implied contract, violation of Maryland's consumer protection statute, unjust enrichment, and for a declaratory judgment. Plaintiff also asserts claims on behalf of himself and various Subclasses described below for violation of numerous state statutes relating to consumer protection, data security, and data breach notification.

8. Plaintiff, individually and on behalf of each of the other members of the Class and Subclasses (defined below), seeks injunctive relief, declaratory relief, monetary and statutory damages, attorneys' fees, and all other relief as may be just and proper as provided under law or by equity.

JURISDICTION AND VENUE

9. This Court has subject-matter jurisdiction pursuant to Courts & Jud. Proc., § 1-501.

10. This Court has personal jurisdiction over Marriott because its principal place of business is located in the State of Maryland, and over Starwood because it is organized under the laws of Maryland. Courts & Jud. Proc., § 6-102(a).

11. Venue properly lies in this Court pursuant to Courts & Jud. Proc., § 6-201(a) because both Marriott and Starwood maintain their respective principal place of business in the State in Montgomery County.

PARTIES

Plaintiff

12. Plaintiff Michael Thomson ("Thomson" or "Plaintiff") is a resident of Bel Air, Maryland in Harford County. Plaintiff has stayed at Starwood and Marriott properties and hotels numerous times in the last four years. Plaintiff is also a member of the Starwood Preferred Guest program ("SPG"), Marriott Rewards program ("Rewards"), owns a time share at a Starwood branded timeshare property, and has both Starwood and Marriott branded credit cards. Plaintiff believes these activities (and possibly others) placed his personal identifying data, and credit card information in the Starwood Guest Reservation database that was compromised in the Data Breach.

13. On December 6, 2018, Plaintiff received notification in three separate emails (4:13 p.m., 4:25 p.m. and 5:20 p.m.) from Marriott that his data had potentially been compromised in the Data Breach.

Defendants

14. Defendant Marriott is a Delaware corporation with its headquarters at 10400 Fernwood Road, Bethesda, Maryland in Montgomery County. Marriott is a worldwide operator, franchisor, and licensor of hotel, residential, and timeshare properties under numerous brand

names at different price and service points. One of the largest hotel chains on the planet, it operates approximately 6,520 properties worldwide, including 4,839 properties in North America alone. On September 23, 2016, Marriott completed the acquisition of Starwood Hotels & Resorts Worldwide, LLC, formerly known as Starwood Hotels & Resorts Worldwide, Inc. through a series of transactions, after which Starwood became an indirect wholly-owned subsidiary of Marriott. Through Starwood, Marriott operates hotels and/or resorts under the Westin, Sheraton, Luxury Collection, Four Points by Sheraton, W Hotels, St. Regis, Le Meridien, Aloft, Element, Tribute Portfolio and Design Hotels brands, as well as other timeshare properties (collectively, the "Starwood Hotels"). Though Marriott's public filings acknowledge that the precise scope of the Data Breach remains uncertain, it is clear that, at a minimum, data pertaining to customers of the Starwood Hotels was compromised in the Data Breach.

15. Defendant Starwood Hotels & Resorts Worldwide, LLC, which is organized under the laws of Maryland, is an indirect wholly-owned subsidiary of Marriott, formerly known as Starwood Hotels & Resorts Worldwide, Inc., which Marriott acquired in September of 2016. Starwood Hotels operated by Marriott include: W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Méridien Hotels & Resorts, Four Points by Sheraton and Design Hotels, as well as Starwood-branded timeshare properties. According to Marriott's Form 8-K filed on November 30, 2018, the Data Breach affected Starwood's legacy customer-reservation database.

STATEMENT OF FACTS

16. Over the past decade and more, a series of high-profile data breaches at major American corporations has highlighted the extreme risks to consumers who share their personal

data to conduct business with such corporations and the corresponding need for those corporations to adopt reasonably solvent means of safeguarding personal data.

17. Personal Information of the type at issue in this action is both private and valuable. Indeed, personal data is so valuable to businesses that a number of applications, including DataWallet, enable consumers to earn money (between $1.00 and $50.00 per transaction) simply by granting access to such information. On the so-called "dark web," personal information of the type at issue here fetches larger amounts, including $20.00 for information pertaining to loyalty accounts, between $5.00 and $110.00 for credit card information, and $1000.00-$2000.00 for passport information.

18. Data breaches of the type at issue in this action present both immediate and ongoing risks to consumers. Hackers or other unscrupulous individuals or organizations may use information of the type compromised by the Data Breach—including, but not limited to, names, phone numbers, email addresses, passport numbers, dates of birth, dates of check-in and departure, and credit card numbers and expiration dates—to, among other things, (i) gain access to individuals' electronic accounts, including social media and bank and credit card accounts, (ii) impersonate consumers in a manner detrimental to their finances or personal reputations, including by creating new accounts without authorization, and (iii) harass, blackmail or otherwise target individuals for fraud or other crimes. Once a breach occurs, consumers whose personal information is used to their detriment are required to undertake costly and time-consuming remedial measures including, among other things, disputing and potentially prosecuting claims regarding contested charges and taking steps to repair damage to credit ratings and other reputational harm. Such consumers also face risks of civil litigation initiated by creditors based on false charges to their accounts.

19. Even if personal information is not used to consumers' detriment upon initially being compromised, consumers remain subject to ongoing risks, requiring them to take various remedial steps lest identity thieves use their Personal Information for nefarious purposes months, years or decades later. These remedial steps, which include, among other things, potentially cancelling accounts, monitoring activity on such accounts, and otherwise remaining vigilant for years or even decades to ascertain whether their information is being used to their detriment, are costly, time-consuming, mentally and emotionally harmful, and nerve-wracking to consumers.

Marriott Knew The Importance of Data Security Prior to the Data Breach

20. Upon information and belief, Marriott maintains electronic databases in which it stores Personal Information divulged by all guests who stay at Marriott properties, including the Starwood Database, which contain information regarding guests who stayed at properties that Marriott has admitted were compromised in the Data Breach. Guests disclose this information to Marriott, among other reasons, for the purposes of making reservations at Marriott-controlled hotels. Guests who disclose this information reasonably expect that Marriott will hold it in confidence and protect it from being compromised.

21. At the time of the Data Breach, Marriott, having observed numerous well-publicized data breaches involving major corporations over the last decade plus, was well aware of the likelihood and repercussions of cybersecurity threats.

22. Indeed, Starwood Hotels, Inc., which Marriott acquired in 2016 and whose system Marriott has identified as having been breached, announced in November of 2015 that databases at 54 of its hotels had been hacked, placing the post-acquisition Marriott on notice of significant security risks at Starwood. The breach was announced in the very same week that Marriott

announced its plan to acquire Starwood for $12.2 billion. Despite this red flag, Marriott did nothing to address the problem.

Marriott Discovers The Data Breach Four Years After at Least One Affected System Was Accessed Without Authorization

23. According to Marriott's November 30, 2018 Form 8-K, "[o]n September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States." In the 8-K, Marriott claims that it "quickly engaged leading security experts to help determine what occurred" and that it "learned during the investigation that there had been unauthorized access to the Starwood network since 2014."

24. According to the 8-K, the Company discovered that "an unauthorized party had copied and encrypted information, and took steps towards removing it." On November 19, 2018, again according to the 8-K, Marriott was able to decrypt the information and determined that the contents were from the Starwood Database.

25. The Company disclosed that it currently believes that the Starwood Database "contains information on up to approximately 500 million guests who made a reservation at a Starwood property" and that "[f]or approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ('SPG') account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences." Masking its potential liability behind a wall of vagueness, the Company also disclosed that "[f]or some, the information also includes payment card numbers and payment card expiration dates[.]" Though the Company noted that the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128), which requires two components for successful decryption, it disclosed that

it had "not been able to rule out the possibility that both were taken." As to the remaining 173 million guests, Marriott vaguely disclosed that the compromised information "was limited to name and sometimes other data such as mailing address, email address, or other information." To date, Marriott has not provided consumers with an explanation of what this "other information" might be, leaving consumers to ponder the precise extent to which their privacy has been invaded.

26. Marriott's President and Chief Executive Officer noted Marriott's "deep regret" of the Data Breach and admitted that Marriott had fallen "short of what our guests deserve and what we expect of ourselves."

Marriott's Conduct Caused Plaintiff and the Members of the Class and Subclasses to Incur Damages

27. Marriott's failure adequately to protect Plaintiff and the members of the Class and Subclasses' Personal Information resulted in devastating injuries and damages.

28. As a direct and proximate result of Marriott's conduct described herein, Plaintiff and the members of the Class and Subclasses have been or will be required to take remedial action, including, but not limited to, freezing, closing or otherwise modifying their credit and other financial accounts, contacting their financial institutions to ascertain the impact of the Data Breach, filing or facing claims regarding contested charges, and reviewing and monitoring credit and other financial reports to detect unauthorized activity.

29. Plaintiff and the members of the Class and Subclasses have thus suffered, and continue to suffer, economic and other damages for which they are entitled to recompense, including:

a. Misappropriation and improper disclosure of their personal and financial information;

b. Unauthorized credit card and other charges;

c. Actual or potential fraud and identity theft;

d. The inability to take adequate remedial measures due to Marriott's unreasonable delay in disclosing the Data Breach;

e. Out-of-pocket expenses arising from their remedial efforts;

f. Diminution in value of their Personal Information;

g. Losses arising from the inability to utilize credit accounts and thus obtain cash-back or other rewards, as well as other damages arising from the inability to use their accounts; and

h. Loss of time due to remedial measures taken.

Marriott's Response to the Data Breach is Insufficient to Make Consumers Whole

30. In response to the Data Breach, Marriott engaged in certain symbolic gestures to give the appearance of trying to make things right.

31. Specifically, in a practical admission of liability, Marriott established a dedicated website and call center to provide consumers with information about the breach, sent email notifications to customers affected by the breach, and offered affected customers the "opportunity" to enroll in an internet monitoring service known as "WebWatcher" free of charge for one year.

32. This is too little, too late. Marriott's customers' data has been compromised for more than four years, meaning that many of the damages arising out of the breach have already occurred. No amount of information or monitoring can address these harms.

33. Further, the mere offer of a years' free monitoring fails to address the fact that Personal Information purloined in the Data Breach will remain extant for multiple years, or even decades.

CLASS ACTION ALLEGATIONS

34. Pursuant to Md. Rule 2-231(a), (b)(2), (b)(3) and (d), Plaintiff seeks certification of the following nationwide class (the "Class" or "Nationwide Class"):

NATIONWIDE CLASS

All persons in the United States whose Personal Information was accessed, compromised, or stolen from Marriott in the Data Breach.

35. Pursuant to Md. Rule 2-231(a), (b)(2), (b)(3) and (d), Plaintiff seeks certification of state-by-state claims in the alternative to the nationwide claims brought under Maryland common law, as well as statutory claims under state data breach statutes and consumer protection statutes, on behalf of separate statewide subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the "Statewide Subclasses" or the "Subclasses"), defined as follows:

STATEWIDE SUBCLASSES

All persons in each of the following States or Territories whose Personal Information was accessed, compromised, or stolen from Marriott in the Data Breach:

Alabama; Alaska; Arizona; Arkansas; California; Colorado; Connecticut; Delaware; District of Columbia; Florida; Georgia; Hawaii; Idaho; Illinois; Indiana; Iowa; Kansas; Kentucky; Louisiana; Maine; Maryland; Massachusetts; Michigan; Minnesota; Missouri; Montana; Nebraska; Nevada; New Hampshire; New Jersey; New Mexico; New York; North Carolina; North Dakota; Ohio; Oklahoma; Oregon; Pennsylvania; Puerto Rico; Rhode Island; South Carolina; South Dakota; Tennessee; Texas; Utah; Vermont; Virginia; Virgin Islands; Washington; West Virginia; Wisconsin; Wyoming.

36. Plaintiff reserves the right to revise the definitions of the Nationwide Class and/or Statewide Subclasses based upon information learned through discovery.

37. Excluded from the Nationwide Class and each State Subclass are Marriott and Starwood, any entity in which either has a controlling interest, and their officers, directors, legal representatives, successors, subsidiaries and assigns. Also excluded from the Nationwide Class

and each Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

38. **Numerosity – Md. Rule 2-231(a)(1).** The members of the Class are so numerous and geographically dispersed that individual joinder of all members of the Class is impracticable. Plaintiff is informed and believes—based upon Marriott's press releases and securities filings—that there are approximately 500,000,000 class members. Those individuals' names and addresses (and in many cases email addresses) are available from Marriott's records, and members of all classes may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, internet postings, and/or published notice. On information and belief, there are at least thousands of class members in each Subclass, making joinder of all Subclass members impracticable.

39. **Commonality and Predominance – Md. Rule 2-231 (a)(2) and 23(b)(3).** This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Class and Subclasses, including, without limitation:

a. Whether Marriott knew or should have known that its computer systems were vulnerable to attack;

b. Whether Marriott failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Marriott failed to take available steps to prevent and stop the Data Breach from happening;

d. Whether Marriott's conduct in connection with the Data Breach breached express or implied contractual obligations to consumers;

e. Whether Marriott represented to Plaintiff and members of the Class and Subclasses that it would safeguard their Personal Information;

f. Whether Marriott failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' Personal Information;

g. Whether Marriott failed to provide timely and adequate notice of the Data Breach to Plaintiff and members of the Class and Subclasses;

h. Whether Marriott owed a duty to Plaintiff and members of the Class and Subclasses to protect Personal Information and to provide timely and accurate notice of the Data Breach to Plaintiff and members of the Class and Subclasses;

i. Whether Marriott breached a duty to protect the Personal Information of Plaintiff and members of the Class and Subclasses by failing to provide adequate data security and by failing to provide timely and accurate notice of the Data Breach to Plaintiff and the members of the Class and Subclasses;

j. Whether Marriott's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems;

k. Whether Marriott's conduct renders it liable for negligence, breach of contract or implied contract, and/or unjust enrichment;

l. Whether Marriott's conduct violated state and territorial consumer protection statutes;

m. Whether Marriott's conduct violated state and territorial statutes governing data privacy and data breach notification;

n. Whether, as a result of Marriott's conduct, Plaintiff and other members of the Class and Subclasses face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

o. Whether, as a result of Marriott's conduct, Plaintiff and other members of the Class and Subclasses are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

40. **Typicality – Md. Rule 2-231 (a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class and Subclasses because, among other things, all members of the Class and Subclasses were comparably injured through Marriott's uniform failures to safeguard their Personal Information and through the Data Breach as described above. The claims of Plaintiff and of the members of the Class and Subclasses arise out of the same nucleus of operative facts and are based on the same legal theories.

41. **Adequacy of Representation – Md. Rule 2-231 (a)(4).** Plaintiff is an adequate class representative because he will fairly and adequately protect the other members of the Class and Subclasses' interests and because his interests do not conflict with their interests. Plaintiff has retained counsel competent and experienced in complex commercial and class action litigation and intends to vigorously prosecute this action. The interests of the other members of the Class and Subclasses will be fairly and adequately protected by Plaintiff and his counsel.

42. **Declaratory and Injunctive Relief – Md. Rule 2-231 (b)(2).** The prosecution of separate actions by individual members of the Class and Subclasses would create a risk of inconsistent or varying adjudications with respect to individual members of the Class and Subclasses that would establish incompatible standards of conduct for Marriott. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other

members of the Class and Subclasses and impair their interests. Marriott has acted and/or refused to act on grounds generally applicable to the members of the Class and Subclasses, making final injunctive relief or corresponding declaratory relief appropriate.

43. **Superiority – Md. Rule 2-231 (b)(3).** Plaintiff and the other members of the Class and Subclasses have all suffered and will continue to suffer harm and damages as a result of Marriott's unlawful and wrongful conduct. A class action is superior to other available means for the fair and efficient adjudication of Plaintiff's and the other members of the Class and Subclasses' claims. While substantial, the damages suffered by each individual Class and Subclass member do not justify the burden and expense of individual prosecution of the complex and extensive litigation required by Marriott's conduct. Even if members of the Class and Subclasses themselves could afford individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation would increase the delay and expense to all parties and the court system given the complex legal and factual issues of this case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

44. The State of Maryland has a significant interest in regulating the conduct of businesses headquartered, or operating within its borders. Maryland, which seeks to protect the rights and interests of Maryland and all residents and citizens of the United States against a company headquartered and doing business in Maryland, has a greater interest in the nationwide claims of Plaintiff and Nationwide Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

45. The principal place of business of Marriott, located at 10400 Fernwood Road, Bethesda, Maryland, is the "nerve center" of its business activities—the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

46. Marriot's decisions relating to its data-protection practices, including its response to the data breach at issue here, and corporate decisions surrounding such response, were made from and in Maryland.

47. Application of Maryland law to the Nationwide Class with respect to Plaintiff's and Class members' claims is neither arbitrary nor fundamentally unfair because Maryland has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the Nationwide Class.

48. Under Maryland's choice of law principles, which are applicable to this action, the common law of Maryland applies to the nationwide common law claims of all Nationwide Class members. Additionally, given Maryland's significant interest in regulating the conduct of businesses operating within its borders, Maryland's Consumer Protection Act may be applied to non-resident consumer plaintiffs.

CLAIMS ALLEGED

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, on Behalf of Plaintiff and the Statewide Subclasses)

49. Plaintiff repeats and re-alleges the allegations contained in Paragraphs 1-48 as if fully set forth herein.

50. Marriott owed a duty to Plaintiff and members of the Class and Subclasses to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting

their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Marriott's security systems to ensure that Plaintiff and the members of the Class and Subclasses' Personal Information in Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

51. Marriott's duty to use reasonable care arose from several sources, including but not limited to those described below.

52. Marriott had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and members of the Class and Subclasses were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and members of the Class and Subclasses would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, but Marriott knew that it was more likely than not that Plaintiff and members of the Class and Subclasses would be harmed.

53. Marriott also acknowledges and recognizes a pre-existing duty to exercise reasonable care to safeguard Plaintiff's and the members of the Class and Subclasses' personal information. As Marriott's President and CEO put it, Marriott's conduct in connection with the Data Breach "fell short of what our guests deserve and what [Marriott] expect[s] of [itself]."

54. Marriott also had a duty to safeguard the Personal Information of Plaintiff and members of the Class and Subclasses and to promptly notify them of a breach because of state

laws and statutes that require Marriott to reasonably safeguard sensitive Personal Information, as detailed herein.

55. Timely notification was required, appropriate and necessary so that, among other things, Plaintiff and members of the Class and Subclasses could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Marriott's misconduct

56. Marriott breached the duties it owed to Plaintiff and the members of the Class and Subclasses described above and thus was negligent. Marriott breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and the members of the Class and Subclasses; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff and the members of the Class and Subclasses' Personal Information in Marriott's possession had been or was reasonably believed to have been, stolen or compromised.

57. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class and Subclasses, their Personal Information would not have been compromised.

58. As a direct and proximate result of Marriott's negligence, Plaintiff and members of the Class and Subclasses have been injured as described herein, and are entitled to damages,

including compensatory, punitive, and nominal damages, in an amount to be proven at trial. These injuries to Plaintiff and the members of the Class and Subclasses include:

a. theft of Personal Information

b. costs associated with credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach— including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;

i. damages to and diminution in value of their Personal Information entrusted, directly or indirectly, to Marriott with the mutual understanding that Marriott would safeguard Plaintiff and the members of the Class and Subclasses' data against theft and not allow access and misuse of their data by others; and

j. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Marriott's possession and is subject to further breaches so long as Marriott fails to undertake appropriate and adequate measures to protect Plaintiff and the members of the Class and Subclasses.

COUNT II
BREACH OF EXPRESS OR IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, on Behalf of Plaintiff and the Statewide Subclasses)

59. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-48 as if fully set forth herein.

60. At all relevant times, Defendants have solicited consumers, including Plaintiff and the members of the Class and Subclasses, to make reservations at hotel properties owned or maintained by Plaintiffs, including Starwood hotels, and have required consumers to provide their Personal Information in the process.

61. When Plaintiff and the members of the Class and Subclasses provided their Personal Information to Defendants when booking rooms or otherwise doing business with Defendants, they entered into express or implied contracts by which Defendants agreed to protect their Personal Information and timely notify them in the event of a data breach.

62. Defendants implicitly and/or affirmatively represented that they collected and stored the Personal Information of Plaintiff and the members of the Class and Subclasses using reasonable, industry standard means.

63. Based on the implicit understanding and also on Defendants' representations (as described above), Plaintiff and the members of the Class and Subclasses accepted Defendants' offers and provided Defendants with their Personal Information.

64. Plaintiff and the members of the Class and Subclasses would not have provided their Personal Information to Defendants had they known that Defendants would not safeguard their Personal Information as promised or provide timely notice of a data breach.

65. Plaintiff and the members of the Class and Subclasses fully performed their obligations under their express or implied contracts with Defendants.

66. Defendants breached the express or implied contracts by failing to safeguard Plaintiff's and the members of the Class and Subclasses' personal information and failing to provide them with timely and accurate notice of the Data Breach.

67. The losses and damages Plaintiff and the members of the Class and Subclasses sustained (as described above) were the direct and proximate result of Defendants' breach of express or implied contracts with Plaintiff and the members of the Class and Subclasses.

COUNT III
VIOLATION OF MD. COMM. CODE §§ 13-301, *et seq.*
("Maryland Consumer Protection Act")
(On Behalf of Plaintiff, the Nationwide Class and the Maryland Subclass)

68. Plaintiff repeats and re-alleges the allegations contained in paragraphs 1-48 as if fully set forth herein.

69. Marriott is a person as defined by Md. Comm. Code § 13-101(h).

70. Marriott's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

71. Plaintiff and members of the Nationwide Class and Maryland Subclass are "consumers" as defined by Md. Comm. Code § 13-101(c).

72. Marriott advertises, offers, or sells "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

73. Marriott advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland, as well as non-residents of Maryland transacting business with Marriott within the state. In advertising, offering or selling goods and services, Marriott represented to the public that it would take reasonable steps to safeguard customers' personal information and failed to disclose the material

fact that it had failed to enact reasonable protective measures with respect to Personal Information disclosed to it by consumers.

74. Marriott engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that consumer goods or services have a characteristic that they do not have;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

d. Failing to state a material fact where the failure deceives or tends to deceive;

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

75. Marriott engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services, in violation of Md. Comm. Code § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff, the Nationwide Class and the Maryland Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Nationwide Class members' Personal Information, including duties imposed by the Maryland Personal Information

Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff, the Nationwide Class and the Maryland Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, the Nationwide Class and the Maryland Subclass members' Personal Information, including duties imposed by the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff, the Nationwide Class and the Maryland Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff, the Nationwide Class and the Maryland Subclass members' Personal Information, including duties imposed by the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

76. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

77. Marriott intended to mislead Plaintiff and members of the Nationwide Class and Maryland Subclass and induce them to rely on its misrepresentations and omissions.

78. Had Marriott disclosed to Plaintiff, the Nationwide Class and the Maryland Subclass that its data systems were not secure and, thus, vulnerable to attack, Marriott's business would have suffered and it would have been forced to adopt reasonable data security measures and comply with the law.

79. Marriott acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff, the Nationwide Class and the Maryland Subclass' rights. Starwood's breach in 2015 put it on notice or, at the very least, inquiry notice that its security and privacy protections were inadequate.

80. As a direct and proximate result of Marriott's unfair and deceptive acts and practices, Plaintiff, the Nationwide Class and the Maryland Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

81. Plaintiff and the members of the Nationwide Class and Maryland Subclass seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, on Behalf of Plaintiff and the Statewide Subclasses)

82. Plaintiff repeats and realleges Paragraphs 1-48, as if fully alleged herein.

83. Plaintiff and members of the Class and Subclasses have an interest, both equitable and legal, in the Personal Information about them that was disclosed to, collected by, and maintained by Marriott and that was compromised in the Data Breach.

84. Marriott was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiff and the members of the Class and Subclasses and by its ability to retain and use that information. Marriott understood that it was in fact so benefitted.

85. Marriott also understood and appreciated that the Personal Information pertaining to Plaintiff and members of the Class and Subclasses was private and confidential.

86. But for Marriott's representation that it was willing and committed to maintaining the privacy and confidentiality of the Personal Information, that information would not have been transferred to and entrusted to Marriott. Further, if Marriott had disclosed that its data security measures were inadequate, Marriott would have faced significant challenges from its shareholders and participants in the marketplace.

87. As a result of Marriott's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and members of the Class and Subclasses without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Marriott has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and members of the Class and the Subclasses. Among other things, Marriott continues to benefit and profit from its use of the Personal Information, while Plaintiff and the members of the Class and Subclasses have been damaged by disclosing it to Marriott.

88. Marriott's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and the members of the Class and Subclasses' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

89. Under the common law doctrine of unjust enrichment, it is inequitable for Marriott to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and members of the Class and Subclasses in an unfair and unconscionable manner.

90. The benefit conferred upon, received, and enjoyed by Marriott was not conferred officiously or gratuitously, and it would be inequitable and unjust for Marriott to retain the benefit.

91. Marriott is therefore liable to Plaintiff and members of the Class and Subclasses for restitution in the amount of the benefit conferred on Marriott as a result of its wrongful conduct.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, on Behalf of Plaintiff and the Statewide Subclasses)

92. Plaintiff repeats and realleges Paragraphs 1-48, as if fully alleged herein.

93. Under the Declaratory Judgment Act, Courts & Jud. Proc. §§ 3-401, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as Marriott's here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

94. An actual controversy has arisen in the wake of the Marriott data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Marriott is currently maintaining data security measures adequate to protect Plaintiff and the members of the Class and Subclasses from further data breaches that compromise their Personal Information. Plaintiff alleges that Marriott's data security measures remain inadequate. Furthermore, Plaintiff and the members of the Class and Subclasses continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

95. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Marriott continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, express or implied contracts between Marriott and consumers, and the various state statutes referred to herein; and

b. Marriott continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

96. The Court also should issue corresponding prospective injunctive relief requiring Marriott to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

97. If an injunction is not issued, Plaintiff and the members of the Class and Subclasses will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Marriott. The risk of another such breach is real, immediate, and substantial. If another breach at Marriott occurs, Plaintiff and the members of the Class and Subclasses will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

98. The hardship to Plaintiff and the members of the Class and Subclasses if an injunction does not issue exceeds the hardship to Marriott if an injunction is issued. Among other things, if another massive data breach occurs at Marriott, Plaintiff and the members of the Class and Subclasses will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Marriott of complying with an injunction by employing reasonable

prospective data security measures is relatively minimal, and Marriott has a pre-existing legal obligation to employ such measures.

99. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Marriott, thus eliminating the additional injuries that would result to Plaintiff, the members of the Class and Subclasses, and the millions of consumers whose confidential information would be further compromised.

COUNT VI
BREACH OF STATE DATA PRIVACY AND NOTICE STATUTES
(On Behalf of the Statewide Subclasses)

100. Plaintiff repeats and realleges Paragraphs 1-48, as if fully set forth herein.

101. According to state laws in the following states and/or territories in which Marriott does business and/or in which Plaintiff and/or members of the Statewide Subclasses reside, Marriott had a duty to implement and maintain reasonable security procedures and/or to timely inform Plaintiff and the Statewide Subclass members of data breaches related to their Personal Information:

a. Alabama: 2018 S.B. 318, Act No. 396 (the "Alabama Data Breach Notification Act")

b. Alaska: Alaska Stat. §§ 45.48.010, *et seq.*; 45.50.471, *et seq.* (the "Personal Information Protection Act")

c. Arizona: Ariz. Rev. Stat. § 18-545, *et seq.*

d. Arkansas: Ark. Code § 4-110-101, *et seq.* (the "Personal Information Protection Act")

e. California; Cal. Civ. Code § 1798.80, *et seq.* (the "California Customer Records Act")

f. Colorado: Colo. Rev. Stat. §§ 6-1-713, *et seq*.; 6-1-716, *et seq*. (the "Colorado Security Breach Notification Act")

g. Connecticut: Conn. Gen. Stat. §§ 42-471; 36a-701b

h. Delaware: 6 Del. Code Ann. §§ 12B-101, *et seq*. (the "Delaware Computer Security Breach Act")

i. District of Columbia: D.C. Code §§ 28-3851, *et seq*. (the "District of Columbia Consumer Security Breach Notification Act")

j. Florida: Fla. Stat. § 501.171

k. Georgia: O.C.G.A. §§ 10-1-910, *et seq*. (the "Georgia Security Breach Notification Act")

l. Hawaii: Haw. Rev. Stat. §§ 487N-1, *et seq*. (the "Hawaii Security Breach Notification Act")

m. Idaho: Idaho Stat. §§ 28-51-104-107

n. Illinois: 815 Ill. Comp. Stat. §§ 530/1, *et seq*. (the "Illinois Personal Information Protection Act")

o. Indiana: Ind. Code § 24-4.9-1-1, *et seq*.

p. Iowa: Iowa Code § 715C.1, *et seq*. (the "Personal Information Security Breach Protection Law")

q. Kansas: Kan. Stat. Ann. §§ 50-6,139b; 50-7a01, *et seq*.

r. Kentucky: Ky. Rev. Stat. Ann. §§ 365.732, *et seq*. (the "Kentucky Computer Security Breach Notification Act")

s. Louisiana: La. Rev. Stat. § 51:3071, *et seq*. (the "Database Security Breach Notification Law")

t. Maine: Me. Rev. Stat. tit. 10 § 1346 *et seq.* (the "Notice of Risk to Personal Data Act")

u. Maryland: Md. Comm. Code §§ 14-3501, *et seq*. (the "Maryland Personal Information Protection Act")

v. Massachusetts: Mass. Gen. Laws § 93H-1 *et seq.*

w. Michigan: Mich. Comp. Laws Ann. §§ 445.72, *et seq*. (the "Michigan Identity Theft Protection Act")

x. Minnesota: Minn. Stat. §§ 325E.61, 325E.64

y. Mississippi: Miss. Code § 75-24-29

z. Missouri: Mo. Rev. Stat. § 407.1500

aa. Montana: Mont. Code Ann. §§ 2-6-1501-1503; 30-14-1704(1), *et seq*.; 33-19-321; (the "Computer Security Breach Law")

bb. Nebraska: Neb.Rev.St. § 87-801, *et seq*. ("Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006")

cc. Nevada: Nev. Rev. Stat. §§ 603A.010 *et seq*., 242.183

dd. New Hampshire: N.H. Rev. Stat. Ann. §§ 359-C:19, *et seq*.

ee. New Jersey: N.J. Stat. Ann. §§ 56:8-161, *et seq*. (the "New Jersey Customer Security Breach Disclosure Act")

ff. New Mexico: 2017 H.B. 15, Chap. 36 (the " Data Breach Notification Act")

gg. New York: N.Y. Gen. Bus. Law § 899-aa (the "Information Security Breach and Notification Act")

hh. North Carolina: N.C. Gen. Stat. § 75-60, *et seq*. (the "North Carolina Identity Theft Protection Act")

ii. North Dakota: N.D. Cent. Code §§ 51-30-01, *et seq.*

jj. Ohio: Ohio Rev. Code §§ 1349.19, *et seq.*

kk. Oklahoma: Okla. Stat. Ann. §§ 24-161-166 (the "Security Breach Notification Act")

ll. Oregon: Or. Rev. Stat. §§ 646A.600, *et seq.* (the "Oregon Consumer Identity Theft Protection Act")

mm. Pennsylvania: 73 Pa. Stat. §§ 2301, *et seq.* (the "Breach of Personal Information Notification Act")

nn. Puerto Rico: P.R. Laws Ann. tit. 10, §§ 4051, *et seq.* (the "Citizen Information on Data Banks Security Act")

oo. Rhode Island: R.I. Gen. Laws §§ 11-49.3-1, *et seq.* (the "Rhode Island Identify Theft Protection Act of 2015")

pp. South Carolina: S.C. Code Ann. §§ 39-1-90, *et seq.* (the "South Carolina Data Breach Security Act")

qq. South Dakota: S.D. Cod. Laws §§ 20-40-20, *et seq.*

rr. Tennessee: Tenn. Code Ann. §§ 47-18-2107, *et seq.* (the "Tennessee Personal Consumer Information Release Act")

ss. Texas: Tex. Bus. & Com. Code § 521.001, *et seq.* (the "Identity Theft Enforcement and Protection Act")

tt. Utah: Utah Code §§ 13-44-101, *et seq.* (the "Protection of Personal Information Act")

uu. Vermont: Vt. Stat. tit. 9 §§ 2430, 2435, *et seq.* (the "Security Breach Notice Act")

vv. Virginia: Va. Code. Ann. §§ 18.2-186.6, *et seq.* (the "Virginia Personal Information Breach Notification Act")

ww. Virgin Islands: V.I. Code tit. 14 §§ 2208, *et seq.* (the "Identity Theft Prevention Act")

xx. Washington: Wash. Rev. Code §§ 19.255.010, *et seq.* (the "Washington Data Breach Notice Act")

yy. West Virginia: W.V. Code §§ 46A-2A-101 *et seq.*

zz. Wisconsin: Wis. Stat. §§ 134.98, *et seq.*

aaa. Wyoming: Wyo. Stat. Ann. §§ 40-12-501, *et seq.*

102. Marriott failed to satisfy its obligations under the foregoing state statutes concerning data breach notification and data privacy restrictions.

103. Timely notification was required, and was appropriate and necessary so that, among other things, Plaintiff and members of the Class and Subclasses could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Marriott's misconduct.

104. Marriott breached the duties it owed to Plaintiff and the members of the Class and Subclasses described above. Marriott breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and the members of the Class and Subclasses; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) timely disclose that Plaintiff and the members of the Class and

Subclasses' Personal Information in Marriott's possession had been or was reasonably believed to have been, stolen or compromised.

105. But for Marriott's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class and Subclasses, their Personal Information would not have been compromised.

106. As a direct and proximate result of Marriott's negligence, Plaintiff and members of the Class and Subclasses have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT VII
BREACH OF STATE CONSUMER PROTECTION STATUTES
(On Behalf of the Statewide Subclasses)

107. Plaintiff repeats and realleges Paragraphs 1-48, as if fully set forth herein.

108. According to state laws in the following states and/or territories in which Marriott does business and/or in which Plaintiff and/or Class members reside, Marriott had a duty to refrain from engaging in unfair, unlawful, fraudulent, abusive and/or deceptive trade practices:

a. Alabama: Ala. Code §§ 8-19-1, *et seq*. (the "Alabama Deceptive Trade Practice Act")

b. Alaska: Alaska Stat. §§ 45.50.471, *et seq*. (the "Alaska Consumer Protection Act")

c. Arizona: Ariz. Rev. Stat. §§ 44-1521, *et seq*. (the "Arizona Consumer Fraud Act")

d. Arkansas: Ark. Code §§ 4-88-107, *et seq*. (the "Arkansas Deceptive Trade Practices Act")

e. California: Cal. Bus. & Prof. Code §§ 17200, *et seq*. (the "California Unfair Competition Law"); Cal. Civ. Code §§ 1750, *et seq*. (the "California Consumer Legal Remedies Act")

f. Colorado: Colo. Rev. Stat. §§ 6-1-101, *et seq*. (the "Colorado Consumer Protection Act")

g. Connecticut: Conn. Gen. St. § 42-110a *et seq.* (the "Connecticut Unfair Trade Practices Act")

h. Delaware: 6 Del. Code § 12-B-102(d), 6 Del. Code § 25 (the "Delaware Consumer Fraud Act")

i. District of Columbia: D.C. Code §§ 28-3904, *et seq.*. (the "District of Columbia Consumer Protection Procedures Act")

j. Florida: Fla. Stat. §§ 501.201, *et seq.* (the "Florida Deceptive and Unfair Trade Practices Act");

k. Georgia: Ga. Code §§ 10-1-370, *et seq.* (the "Georgia Uniform Deceptive Trade Practices Act")

l. Hawaii: Haw. Rev. Stat. §§ 480-1, *et seq.* (the "Hawaii Unfair Practices and Unfair Competition Act"); Haw. Rev. Stat. §§ 481A-3, *et seq.* (the "Hawaii Uniform Deceptive Trade Practice Act")

m. Idaho: Idaho Code §§ 48-601, *et seq.* (the "Idaho Consumer Protection Act")

n. Illinois: 815 Ill. Comp. Stat. §§ 505, *et seq.* (the "Illinois Consumer Fraud Act"); 815 Ill. Comp. Stat. §§ 510/2, *et seq.* (the "Illinois Uniform Deceptive Trade Practices Act")

o. Indiana: Ind. Code §§ 24-5-0.5-1, *et seq.* (the "Indiana Deceptive Consumer Sales Act")

p. Iowa: Iowa Code § 714H (the "Iowa Private Right of Action for Consumer Frauds Act")

q. Kansas: Kan. Stat. §§ 50-623, *et seq.* (the "Kansas Consumer Protection Act")

r. Kentucky: Ky. Rev. Stat. §§ 367.110, *et seq.* (the "Kentucky Consumer Protection Act")

s. Louisiana: La. Rev. Stat. §§ 51:1401, *et seq.* (the "Louisiana Unfair Trade Practices and Consumer Protection Law")

t. Maine: 5 Me. Rev. Stat. §§ 205, 213, *et seq.* (the "Maine Unfair Trade Practices Act"); 10 Me. Rev. Stat. §§ 1212, *et seq.* (the "Maine Uniform Deceptive Trade Practices Act")

u. Maryland: Md. Code Com. Law §§ 13-301, *et seq.* (the "Maryland Consumer Protection Act")

v. Massachusetts: Mass. Gen. Laws ch. 93A, §§ 1, *et seq.* (the "Massachusetts Consumer Protection Act")

w. Michigan: Mich. Comp. Laws §§ 445.903, *et seq.* (the "Michigan Consumer Protection Act")

x. Minnesota: Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.* (the "Minnesota Consumer Fraud Act"); Minn. Stat. §§ 325D.43, *et seq.* (the Minnesota Uniform Deceptive Trade Practices Act");

y. Mississippi: Miss. Code §§ 75-24-1, *et seq.* (the "Mississippi Consumer Protection Act")

z. Missouri: Mo. Rev. Stat. §§ 407.010, *et seq.* (the "Missouri Merchandise Practices Act")

aa. Montana: Mont. Code §§ 30-14-101, *et seq.* (the "Montana Unfair Trade Practices and Consumer Protection Act")

bb. Nebraska: Neb. Rev. Stat. §§ 59-1601, *et seq.* (the "Nebraska Consumer Protection Act"); Neb. Rev. Stat. §§ 87-301, *et seq.* (the "Nebraska Uniform Deceptive Trade Practices Act")

cc. Nevada: Nev. Rev. Stat. §§ 598.0903, *et seq.* (the "Nevada Deceptive Trade Practices Act")

dd. New Hampshire: N.H. Rev. Stat. §§ 358-A, *et seq.* (the "New Hampshire Consumer Protection Act")

ee. New Jersey: N.J. Rev. Stat. §§ 56:8-1, *et seq.* (the "New Jersey Consumer Fraud Act")

ff. New Mexico: N.M. Stat. §§ 57-12-2, *et seq.* (the "New Mexico Unfair Practices Act")

gg. New York: N.Y. Gen. Bus. Law §§ 349, *et seq.* (the "New York General Business Law")

hh. North Carolina: N.C. Gen. Stat. §§ 75-1.1, *et seq.* (the "North Carolina Unfair Trade Practices Act")

ii. North Dakota: N.D. Cent. Code §§ 51-15-01, *et seq.* (the "North Dakota Unlawful Sales or Advertising Act")

jj. Ohio: Ohio Rev. Code §§ 4165.01, *et seq.* (the "Ohio Deceptive Trade Practices Act")

kk. Oklahoma: Okla. Stat. tit. 15, §§ 751, *et seq.* (the "Oklahoma Consumer Protection Act")

ll. Oregon: Or. Rev. Stat. §§ 646.608, *et seq.* (the "Oregon Unlawful Trade Practices Act")

mm. Pennsylvania: 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.* (the "Pennsylvania Unfair Trade Practices and Consumer Protection Law")

nn. Puerto Rico: 10 P.R. Laws §§ 257, *et seq.* (the "Puerto Rico Fair Competition Law")

oo. Rhode Island: R.I. Gen. Laws §§ 6-13.1, *et seq.* (the "Rhode Island Deceptive Trade Practices Act")

pp. South Carolina: S.C. Code §§ 39-5-10, *et seq.* (the "South Carolina Unfair Trade Practices Act")

qq. South Dakota: S.D. Codified Laws §§ 37-24-1, *et seq.* (the "South Dakota Deceptive Trade Practices and Consumer Protection Law")

rr. Tennessee: Tenn. Code §§ 47-18-101, *et seq.* (the "Tennessee Consumer Protection Act")

ss. Texas: Texas Bus. & Com. Code §§ 17.41, *et seq.* (the "Deceptive Trade Practices—Consumer Protection Act")

tt. Utah: Utah Code §§ 13-11-1, *et seq.* (the "Utah Consumer Sales Practices Act")

uu. Vermont: Vt. Stat. Ann. Tit. 9, §§ 2451, *et seq.* (the "Vermont Consumer Fraud Act")

vv. Virginia: Va. Code §§ 59.1-196, *et seq.* (the "Virginia Consumer Protection Act")

ww. Virgin Islands: V.I. Code tit. 12A, §§ 301, *et seq.* (the "Virgin Islands Consumer Fraud and Deceptive Business Practices Act"); V.I. Code tit. 12A, §§101, *et seq.* (the "Virgin Islands Consumer Protection Law")

xx. Washington: Wash. Rev. Code §§ 19.86.020, *et seq.* (the "Washington Consumer Protection Act")

yy. West Virginia: W. Va. Code §§46A-6-101, *et seq.* (the "West Virginia Consumer Credit and Protection Act")

zz. Wisconsin: Wis. Stat. § 100.18 (the "Wisconsin Deceptive Trade Practices Act")

aaa.

a. Wyoming: Wyo. Stat. § 40-12-101, *et seq*. (the "Wyoming Consumer Protection Act"))

109. Marriott failed to satisfy its obligations under the foregoing state statutes concerning unfair, unlawful, abusive and deceptive trade practices and consumer protection restrictions.

110. Marriott engaged in unfair, unlawful, abusive and deceptive trade practices in connection with offering for sale or selling consumer goods or services, in violation of the foregoing statutes, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the Statewide Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Marriott data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Statewide Class members' Personal Information, which was a direct and proximate cause of the Marriott data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the Statewide Class members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the Statewide Class members' Personal Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the Statewide Class members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Statewide Class members' Personal Information.

111. Marriott's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Marriott's data security and ability to protect the confidentiality of consumers' Personal Information. Marriott's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

112. Marriott intended to mislead Plaintiff and members of the Statewide Classes and induce them to rely on its misrepresentations and omissions.

113. Had Marriott disclosed to Plaintiff and the members of the Statewide Classes that its data systems were not secure and, thus, vulnerable to attack, Marriott's business would have suffered and it would have been forced to adopt reasonable data security measures and comply with the law.

114. Marriott acted intentionally, knowingly, and maliciously to violate the foregoing state consumer protection statutes, and recklessly disregarded Plaintiff and the members of the Statewide Classes' rights. Starwood's previous breach put it on notice or, at the very least, inquiry notice that its security and privacy protections were inadequate.

115. As a direct and proximate result of Marriott's unfair, unlawful and deceptive acts and practices, Plaintiff and the members of the Statewide Classes have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

116. Plaintiff and the members of the Statewide Classes seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class and Subclasses, respectfully requests the following relief:

a. that this Court certify this action as a class action pursuant to Md. Rule 2-231(a), (b)(2) and (b)(3), and appoint Plaintiff as Class representative and his counsel as Class Counsel;

b. that this Court enter judgment in favor of Plaintiff and the other members of the Class and Subclasses, and against Defendant Marriott under the legal theories alleged herein;

c. that Marriott's wrongful conduct alleged herein be adjudged and decreed to violate the Data Protection and Data Breach Notice Statutes as asserted and that the Court issue an order enjoining the methods, acts, or practices adjudged and decreed unlawful

d. that Marriott's wrongful conduct alleged herein be adjudged and decreed to violate the Deceptive Trade Practice Statutes as asserted and that the Court issue an order enjoining the methods, acts, or practices adjudged and decreed unlawful;

e. that Plaintiff and each of the other members of the Class and Subclasses be awarded their actual damages and, where applicable, statutory or other damages, with pre- and post-judgment interest, as provided by law;

f. that Plaintiff and each of the other members of the Class and Subclasses recover their costs of suit, including reasonable attorneys' fees and expenses as provided by law; and

g. that Plaintiff and each of the other members of the Class and Subclasses be granted such other and further relief as the nature of the case may require or as this Court deems just and proper.

JURY DEMAND

117. Plaintiff, individually and on behalf of the other members of the Class and Subclasses, demands a trial by jury on all issues so triable.

Dated: December 12, 2018

Respectfully submitted,

GRANT & EISENHOFER P.A.
Jay W. Eisenhofer (*pro hac vice* to be filed)
Kyle J. McGee (*pro hac vice* to be filed)
Michael D. Bell (*pro hac vice* to be filed)
123 Justison Street
Wilmington, Delaware
Tel: 302-622-7000
Fax: 302-622-7100
jeisenhofer@gelaw.com
kmcgee@gelaw.com
mbell@gelaw.com

GORDON, WOLF & CARNEY, CHTD.
Martin E. Wolf
Richard S. Gordon
Benjamin H. Carney
100 W. Pennsylvania Ave., Suite 100
Towson, Maryland 21204
Tel: 410-825-2300
Fax: 410-825-0066
mwolf@GWCfirm.com
rgordon@GWCfirm.com
bcarney@GWCfirm.com

By: ______________________

Attorneys for Plaintiff, Class, and Subclasses